(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 537 098 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
13.01.1999 Bulletin 1999/02

(51) Int Cl.6: G06F 11/34

(21) Application number: 92480124.4

(22) Date of filing: 11.09.1992

(54) Event handling mechanism having a filtering process and an action association process

Ereignisbehandlungsvorrichtung mit Filterverfahren und mit Einwirkungassoziationsverfahren

Dispositif de traitement d'événement à procédés de filtrage et d'association d'action

(84) Designated Contracting States:
DE FR GB

(30) Priority: 11.10.1991 US 775669

(43) Date of publication of application:
14.04.1993 Bulletin 1993/15

(73) Proprietor: International Business Machines Corporation
Armonk, N.Y. 10504 (US)

(72) Inventors:
- Daniel, Arthur Aulden
Rochester, Minnesota 55902 (US)
- McKelvey, Mark Ambrose
Rochester, Minnesota 55902 (US)
- Modry, John Arthur
Rochester, Minnesota 55901 (US)
- Roubal, Eric Gunter
Rochester, Minnesota 55901 (US)
- Sandstrom, Andrew Edward
Rochester, Minnesota 55904 (US)
- Wildt, Patrick Michael
Rochester, Minnesota 55901 (US)

(74) Representative: de Pena, Alain et al
Compagnie IBM France
Département de Propriété Intellectuelle
06610 La Gaude (FR)

(56) References cited:
WO-A-89/07795 WO-A-93/00632

- PATENT ABSTRACTS OF JAPAN vol. 11, no. 342 (P-635)10 November 1987 & JP-A-62 125 402 (YOKOGAMA ELECTRIC CORP.) 6 June 1987
- IBM TECHNICAL DISCLOSURE BULLETIN. vol. 34, no. 5 , October 1991 , NEW YORK US pages 415 - 417 XP189771 'Process for Real-Time, Trace-driven Performance Monitors'
- ELECTRONIQUE INDUSTRIELLES no. 86, 1 April 1985 , PARIS FR pages 54 - 58 A. PERREUR 'L'optimisation de logiciels à l'aide de diagrammes et histogrammes d'événements'

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

This invention relates to the data processing field. More specifically, this invention is an event handling mechanism that categorizes the events of a raw event stream into groups of events and associates an action or actions with each group.

BACKGROUND OF THE INVENTION

The system software of today's single and multiple processor environments usually includes a crude event handling mechanism. The purpose of this mechanism is to provide some degree of control for the potentially large amount of event traffic on the system's communication networks. It is the responsibility of an event handling mechanism to route and/or coordinate the event traffic to best utilize the resources of the system. Existing event handler implementations perform various operations on an event stream. Examples include the deletion, logging, and/or display of certain events, usually on a system console monitored by a system administrator. These event handlers are "hard coded" to handle particular events and particular streams of events. When new events are added to an event stream, major modifications to the event handler must in turn be made to accommodate them. In some cases an entire new event handler is required. A new event handler is almost always required whenever support for a new or different event stream protocol is desired. This situation is further complicated when one considers a system that supports multiple event streams and thus includes multiple event handlers. In this latter system, the addition of a newly supported protocol not only means that a new event handler is required, but it also means that the software that coordinates the event handlers must also be rewritten.

The result of the cost and complexity associated with these modifications is the inability to provide significant function to the end user (e.g., system administrator). For the most part, the example functions cited above (i.e., deletion, logging, and display on a system console) typify current event handler implementations. This limited function in turn results in several problems: entire categories of events must be deleted to accommodate more important categories, some events are never seen because the system console is unattended when an event appears, and logs are so large that it is difficult to detect events of significance. In general, this makes the system administrator task more difficult because that person has only limited control over a large portion of the information necessary to perform their job.

An article of the IBM TDB vol.34 no.5 October 1991, page 415-417, relates to a process for real time, trace-driven performance monitors. This process is driven by a "trace" or log of system events, such as the traces that are available in the AIX operating system (IBM registered trademarks).

An international application WO 93 /00632, published on 07.01.93 and falling within the terms of Article 54(3) EPC, relates to a method and system for monitoring and changing the operation of a computer system which comprises a plurality of computers in a local area network or a plurality of interconnected local area network. The monitoring and changing may concern error processing for instance error detecting, registering and rectifying occurring during the operation of a computer system. In this process, the method and system consist in using at least one event report generator in each program which is executable in the computer system and whose execution is monitored depending on a flexible rule base which is included in an event processing machine and which associates a certain event with a predetermined action for determining the action associated with the reported event. But the techniques disclosed therein does not enable to reduce the cost management of a computer system's event streams.

US Patent Application US-A-4 965 772 (Daniel et al.) entitled "Method and Apparatus for Communication Network Alert Message Construction" discloses construction and display of operator messages representative of alert conditions in a network. Code points, which are strings of bits, are generated in response to an event in a device attached to the network. The code points are used to index predefined tables that contain relatively short units of text messages in operator selectable languages to be used in building an operator's information display. A product attached to a network, an alert sender, will generate a series of code points representative of desired display messages for an operator. The messages are independent of the specific alert sending product insofar as an alert receiver is concerned. The operator can also choose between detailed and general display messages. The code points are hierarchically arranged so that if the alert receiver does not have the most up to date set of messages, the alert receiver will display a more generic message which is still represenattaive of the event.

SUMMARY OF THE INVENTION

It is a principle object of this invention to provide for the effective, efficient, and cost reduced management of a computer system's event streams.

It is another object of this invention to provide the system administrator with the ability to dynamically categorize and re-categorize the events of a system's event stream(s).

It is still another object of this invention to provide the system administrator with the ability to dynamically modify how the system processes particular events or groups of events without having to change how the events have been categorized.

These and other objects are accomplished by the event handler mechanism laid down in the independent claims. Further enhancements are provided by the subclaims.

Computer systems have the ability to monitor their components and operations, generate events which indicate the occurrence of a monitored condition (e.g. out of paper, Joe Smith just signed on, disk utilization nearing capacity, etc.), and process these events in some manner.

The present invention provides significant enhancements to the latter capability.

The events of an event stream or streams are "filtered" into categories or groups of events. Once categorized, the invention associates an action or actions with the categorized event. The associated action can be logging the event, routing the event to the electronic address of a user, or sending the event to an application program for further processing.

The filtering process is accomplished through the use of four discrete components: a filter table, a filter table maintenance mechanism, a parsing mechanism, and a filter table processing mechanism. The filter table is maintained by the system administrator, and contains a plurality of filter entries. The filter entries in turn contain a sequence number, a group identifier, and certain selection criteria. The selection criteria includes a collection of element types, values, and operators. The system administrator uses the filter table maintenance mechanism to create, modify, and delete both the filter entries and the filter table itself. In doing so, the system administrator is given the ability to categorize all events of an event stream.

The parsing mechanism parses out select elements of each event contained in a raw event stream. These elements then comprise a standardized event. The parsing mechanism produces the same standardized event regardless of the form of the events in the raw event stream. The filter table processing mechanism then takes the selection criteria of the filter entries and applies them to the element types and values of the standardized event. If a match is detected, the group identifier is passed to the action mechanism of the invention. If not, a default group identifier is passed on.

The action mechanism of the invention entails three discrete components: an action table, an action table maintenance mechanism, and an action table processing mechanism. The action table is maintained by the system administrator. The action table contains a plurality of group entries. The group entries are used when groups are provided by the filtering process discussed above, or when an application program supplies categorized events to this portion of the invention. The group entries contain a group identifier and associated actions, such as routing the event to an electronic address or another application program.

The system administrator will use the action table maintenance mechanism to create, modify, and delete the group entries, event entries and the action table itself. In doing so, each event or group of events will be acted upon in the same manner.

In operation, the action table processing mechanism will attempt to match the subject group or event with a group or event entry in the action table. If there is a match, the action table processing mechanism will route the event to an application program or the electronic address of one or more end users. If there is not a match, the action table processing mechanism will route the event to a default destination such as the system console or "bit bucket".

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows the computer system of the invention.

Fig. 2 shows the process flow of the preferred embodiment.

Fig. 3 shows the two logical functions of the preferred embodiment and their interaction with the system administrator.

Fig. 4 shows the process flow of the filter table and action table maintenance mechanisms of the preferred embodiment.

Figs. 5 and 7 depict the user interface of the preferred embodiment.

Figs. 6 and 8 show how the user's input is manipulated after its entry.

Fig. 9 shows the table structure of the invention.

Fig. 11 shows an example event that could be handled by the invention.

Fig . 12 shows an exemplary result of the initial parsing step.

Figs. 10, 13, and 14 are flow diagrams describing the processes of the preferred embodiment.

Fig. 15 depicts an alternate embodiment of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Fig. 1 shows a block diagram of the computer system 10 of the invention. Computer system 10 contains storage 11, CPU 12, memory 13, event monitor 14, event generator 15, event handler 16, and communications interface 20. Although the discussion of the preferred embodiment focuses on events received from communications interface 20, it is important to note that the invention also applies equally to events received from other internal entities that are capable of generating events.

Fig. 1 also shows connections to other computer systems 21 via communications line 22. The invention itself is located in event handler 16. Event handler 16 contains filter mechanism 17, action mechanism 18, and editor 19.

In the preferred embodiment, computer system 10 is an Application System/400 (IBM registered trademark) midrange computer system, although other computer systems such as personal computers and mainframe computer systems could also be used. In addition, communications line 22 could be a direct connection cable, a local area network, telecommunications link, or other form of operatively connecting computers together.

Referring now to Fig. 2, events 25 are shown as input to event handler 16 of the invention. Events 25 could represent any type of event stream. All possible events that can be generated by event generator 15 and sent to event handler 16 in a continuous or discontinuous fashion as computer system 10 is operating will be referred to herein as an event stream. When each event encounters filter 17, it is labeled as being a member of a particular event group 27. The invention then uses the event group label (event group 27) and action table 28 to decide what actions 29 are appropriate for this event 25. The various actions 29 are then performed by the system.

Fig. 3 shows event handler 16 in more detail. As mentioned above, the events of raw event stream 25 first encounter filter mechanism 17. The filter process 34 uses a filter table 32 to filter (or label as mentioned above) the events into an event group 35. Filter table 32 contains filter entries 33. These filter entries are used to determine which event group is appropriate for the subject event. Once this determination is made, event group 35 is passed on to action process 39. To decide what actions are required, the action process 39 compares the group entries 38 of the action table 37 to the event group 35. Action executer 41 then uses this information to execute the actions.

Fig. 3 further depicts the ability of the system administrator 36 to create and modify the filter table 32 and the action table 37. A "system administrator" referred to herein is normally one or more persons responsible for the continued operation of computer system 10. If computer system 10 is a personal computer, the user of the personal computer or the person responsible for the continued operation of the local area network would be considered to be the system administrator. Fig. 4 describes this ability in more detail.

Referring now to Fig. 4, the system administrator would first elect to work with the event handler function 40. The system administrator can choose which filter to work with and what type of filter he or she would like it to be. These choices are significant in that they give the system administrator control over what filters are used for what purposes. This flexibility is important because the event handler of the preferred embodiment utilizes different filter tables in different situations. Next, the system administrator must elect to work with the action table 49 or work with the filter table 42. Once the choice has been made, the system administrator can create , change, delete, or print either of the two logical constructs (i.e. the filter table or the action table). Another option at this level is the ability to perform operations on the entries of either of the logical constructs 44 and 45. An entry can be added, copied, changed, removed, displayed , or renamed, 46 and 47.

Fig. 5 depicts the screen that is seen when the system administrator elects to work with the filter table's entries. Each filter entry contains a sequence number 50, a group identifier (group 51), and selection criteria (selection data 52). Sequence number 50 is used to control the order in which the filter table is searched. Group identifier 51 represents the category in which events can be placed. The selection criteria 52 is used to determine the category in which the subject event belongs. It does so, by using the elements of each event. In particular, the selection criteria is used to determine whether an event's element types and the associated values satisfy the test set forth in the selection criteria itself. Boolean expressions which include relational operators, Boolean operators, or both are used to create the "test" of the selection criteria.

Fig. 6 depicts the expression flow of the screen shown in Fig. 5. The add filter entry function 60 converts the user information into a device specific data format 63. In the preferred embodiment, the use of the add filter entry function 60 results in the information being parsed 61 and then converted into an optimized form 62. The preferred embodiment uses a generic parser which first converts the expression into an infix binary expression tree containing relational and Boolean operators. The filter table parser then converts the tree into a prefix data stream for high performance string-based evaluation. The device specific data format 63 is a single stream prefix expression that contains a length, a Boolean or relational operator, and the right and left sub-expressions recursively listed. The single stream representation containing lengths and recursive expressions allows for optimized evaluations by reducing the number of sub-expression evaluations needed. It is in this fashion that the system administrator's categorization scheme is represented in the filter table 64.

Fig. 7 depicts the screen that is seen when the system administrator elects to work with the action table's entries. Each action table entry contains a group identifier (group 70) and at least one associated action 71. Associated actions can be routing the event to one or more electronic addresses of specific users, logging the event in a specific log, or sending the event to an application program , as shown in Fig. 7.

Fig. 8 depicts the expression flow of the screen shown in Fig. 7. In the preferred embodiment, the use of the add group entry function 80 results in the information being converted into a generic form 81 and then into an optimized form 82. The data's resultant form is device specific 83.

It is in this fashion that the system administrator's action association scheme is represented in action table 84. In the preferred embodiment, the add group entry function 80 converts the specific action (parameter) information 85 into generic actions ((action 1, parameter 1)...(action N, parameter N)) format 81. The generic format 81 allows the add group entry function 80 to convert any action into the internal device specific data 83.

The internal device representation 83 identifies the data as a group entry which identifies the group (category), and lists the actions and parameters.

Fig. 9 shows the combined filter table/action table structure 90 of the preferred embodiment. Though it is conceptually easier to think of the filter table and action table as separate data structures, they are actually combined into a single data structure in the preferred embodiment. In the preferred embodiment, keys for filter 93 and group entries 92 are placed in index 91. When retrieval is needed, the offsets in the index are used to gain access to the data area 94 where the data 95 is stored.

Fig. 10 depicts the four conceptual entities of the filter process (first described as the filter function at 17 in Fig. 1). The filter processing and filter maintenance mechanism (103, 106) were explained in the discussion of Figs. 4, 5, 6. The parsing mechanism 101 is responsible for convert ing the raw data events 100 into standardized events 102. The event of Fig. 11 is an example of what an event could look like prior to parsing. As was mentioned in the discussion of Fig. 5, the filter table's selection criteria is primarily concerned with the event's element types 111 and the associated values 112. Hence, it is the parsing mechanism's task to parse out the important elements and assign them a type. It is particularly important that this is done consistently regardless of the type of event received. An example is shown in Fig. 12 where only those elements that are actually needed are placed into the standardized event. Returning now to Fig.10, it is seen t hat the standardized event is presented to the filter processing mechanism 103. The filter processing mechanism 103 will use the selection criteria of the filter entries from filter table 105 to discern a match. Once accomplished, the filter processing mechanism 103 will pass the group identifier (event group 104) to the action processing function.

Fig. 13 describes action processing (first described as action mechanism 18 in Fig. 1). The action table processing and action table maintenance mechanism (131, 134) were described in the discussion regarding Figs. 4, 7, and 8. The action table processing mechanism 131 uses the event group passed to it by the filter table processing mechanism to locate the appropriate action 132 contained in the action table 133. Once located, the action table processing mechanism 131 passes the action 132 on to be executed as indicated.

Fig. 14 is a flow diagram that shows the steps used by the filter processing 148 and the action table process ing 149 mechanisms and how the two mechanisms interact. The filter processing mechanism begins by retrieving the first filter entry at block 140. The filter processing mechanism will the n traverse the expression tree of Fig. 6 and attempt to locate a match 141. If a match is achieved, the associated group identifier is passed to the action table processing mechanism 149. If a match is not found, the next filter entry is retrieved at block 143 and the process is repeated. If a match is not achieved before the last filter entry is evaluated, a default group identifier (which automatically "matches" events not matched by other entries) is used. When the action table processing mechanism 149 receives the group identifier, it will attempt to locate the correct group entry in the action table 144. If the group identifier exists within the action table, the associated action is executed by block 147. If the group identifier does not exist within the action table, a default entry is used in block 146. This results in a default action being passed on to block 147.

Fig. 15 depicts one possible alternate embodiment. In this embodiment, a filter process could be used without the companion action processing. The application program 150 would receive the event groups 152 directly and perform both the action association function and action execution function. Although this embodiment does not provide the flexibility of the preferred embodiment, it still represents an improvement over existing implementations. The system administrator 151 retains the flexibility of being able to control how events are to be categorized.

Claims

1. A method for handling events in a data processing system's event stream (25), said method comprising the steps of:

   accepting as input a user created categorization scheme, said user created categorization scheme being used to construct a filter table (32) receiving as input said events;

   applying said events to said filter table; and

   categorizing said events into groups of events based on a comparison of characteristics of said events with information contained in said filter table.

2. The method of claim 1 wherein the accepting step of said user categorization scheme further comprises the steps of:

   accepting as input a modified user categorization scheme; and

   parsing said user input into a device specific representation.

3. The method of claim 2 wherein said accepting step further comprises the step of:

   inputting a plurality of sequentially arranged filter entries (33) into said filter table (32).

4. The method of claim 3 wherein said inputting step further comprises the step of:

adding a group identifier, a sequence number, and a set of selection criteria to each of said filter entries.

5. The method of claim 4 wherein said adding step further comprises the step of:

entering, as part of said selection criteria a set of element types, values, and operators.

6. The method of claim 5 where in said entering step further comprises the step of:

placing a wild card character identifier into said value.

7. The method of claim 1 wherein said applying step further comprises the step of:

parsing said events into standardized events.

8. The method of claim 6 wherein said categorizing step further comprises the steps of:

using said sequence numbers to search through said filter entries;

matching said element types and said values to a particular element's type and value; and

interpreting said wild card character identifiers.

9. The method of any one of the previous claims further comprising the steps of:

accepting as input a user created action association scheme, said action association scheme being used to construct an action table (37);

receiving as input an event group;

applying said event group to said action table to determine said particular actions, said particular actions being determined by comparing characteristics of said event group with information contained in said action table; and

outputting said particular actions to an application program for further processing.

10. The method of claim 9 wherein said outputting step further comprises:

sending said particular actions to a person located at an electronic address on a computer system.

11. The method of claim 9 wherein said action table construction step further comprises the steps of:

accepting user input to create and modify said action association scheme; and

parsing said user input into a device specific representation.

12. The method of claim 11 wherein said action table construction step further comprises the step of:

inputting a plurality of group entries into an action table.

13. The method of claim 12 wherein said group entries inputting step further comprises the step of:

adding a group identifier and actions to each of said group entries.

14. The method of claim 13 wherein said action determining step further comprises the steps of:

using said group identifiers to search through said group entries: and

matching said group identifier to a particular group's type.

15. An apparatus for handling events in a data processing system's event stream (25), said apparatus comprising:

means for accepting as input a user created categorization scheme, said user created categorization scheme being used to construct a filter table (32) receiving as input said events;

means for applying said events to said filter table: and

means for categorizing said events into groups of events based on a comparison of characteristics of said events with information contained in said filter table (32).

16. The apparatus of claim 15 wherein said means for accepting said user categorization scheme further comprises:

means for accepting user input to construct and modify said categorization scheme.

17. The apparatus of claim 16 wherein said means for accepting user input further comprises:

means for parsing said user input into a device specific representation.

18. The apparatus of claim 17 wherein said filter table comprises a plurality of sequentially arranged filter entries (33), each of said filter entries comprising a group identifier, a sequence number, and a set of selection criteria.

19. The apparatus of claim 18 wherein said set of selection criteria comprises a set of element types, values, and operators,. said operators being relational

20. The apparatus of claim 19 wherein said operators are Boolean.

21. The apparatus of claim 20 wherein said value comprises a wild card character identifier.

22. The apparatus of claim 15 wherein said means for accepting user input further comprises:

means for parsing said events into standardized events.

23. The apparatus of claim 21 wherein said means for applying further comprises:

means for using s aid sequence numbers to search through said filter entries;

means for matching said element types and said values to a particular element's type and value; and

means for interpreting said wild card character identifiers.

24. The apparatus according to any one of claims 15 to 23 further comprising:

means for accepting as input a user created action association scheme, said action association scheme being used to construct an action table (37);

means for receiving as input an event group;

means for applying said event group to said action table to determine said particular actions, said particular actions being determined by comparing characteristics of said event group with information contained in said action table; and

means for outputting said particular actions to an application program for further processing.

25. The apparatus of claim 24 wherein a destination of said means for outputting is a person located at an electronic address on a computer system.

26. The apparatus of claim 24 wherein said action table construction means further comprises means for:

accepting user input to create and modify said action association scheme; and

parsing said user input into a device specific representation.

27. The apparatus of claim 26 wherein said action table construction means further comprises means for:

inputting a plurality of group entries into an action table.

28. The apparatus of claim 27 wherein said means for inputting group entries further comprises means for:

adding a group identifier and actions to each of said group entries.

29. The apparatus of claim 28 wherein said means for determining said particular actions further comprises means for:

using said group identifiers to search through said group entries; and

matching said group identifier to a particular group.

Patentansprüche

1. Eine Vorrichtung zur Ereignisbehandlung in einem Ereignisstrom (25) eines Datenverarbeitungssystems, folgende Schritte umfassend:

Akzeptieren eines von einem Benutzer eingegebenen Kategorisierungsschemas als Eingabe, wobei das genannte vom Benutzer erstellte Kategorisierungsschema zur Erstellung einer Filtertabelle (32) verwendet wird, die als Eingabe die genannten Ereignisse erhält;

Anwenden der genannten Ereignisse auf die genannte Filtertabelle; und

Kategorisieren der genannten Ereignisse in Gruppen, basierend auf dem Vergleich von Eigenschaften der genannten Ereignisse mit in der genannten Filtertabelle enthaltenen Daten.

2. Eine Methode nach Anspruch 1, bei der der Schritt des Akzeptierens des genannten vom Benutzer erstellten Kategorisierungsschemas weiterhin folgende Schritte umfaßt:

   Akzeptieren eines geänderten Benutzer-Kategorisierungsschemas als Eingabe; und

   Syntaktisches Analysieren der genannten Benutzereingabe in einer gerätespezifischen Darstellung.

3. Eine Methode nach Anspruch 2, bei der der genannte Schritt des Akzeptierens weiterhin folgenden Schritt umfaßt:

   Aufnehmen einer Vielzahl von sequentiell angeordneten Filtereingaben (33) in die genannte Filtertabelle (32).

4. Eine Methode nach Anspruch 3, bei der der genannte Schritt der Aufnahme weiterhin folgenden Schritt umfaßt:

   Hinzufügen einer Gruppenkennung, einer Sequenznummer und eines Satzes an Auswahlkriterien zu jeder der genannten Filtereingaben.

5. Eine Methode nach Anspruch 4, bei der der genannte Schritt des Hinzufügens weiterhin folgenden Schritt umfaßt:

   Eingeben eines Satzes an Elementtypen, Werten und Operatoren als Teil der genannten Auswahlkriterien.

6. Eine Methode nach Anspruch 5, bei der der genannte Schritt der Eingabe weiterhin folgenden Schritt umfaßt:

   Plazieren einer Platzhalterkennung in den genannten Wert.

7. Eine Methode nach Anspruch 1, bei der der genannte Schritt des Anwendens weiterhin folgenden Schritt umfaßt:

   Syntaktisches Analysieren der genannten Ereignisse in standardisierte Ereignisse.

8. Eine Methode nach Anspruch 6, bei der der genannte Schritt des Kategorisierens weiterhin folgende Schritte umfaßt:

   Verwenden der genannten Sequenznummern zum Durchsuchen der genannten Filtereingaben;

   Anpassen der genannten Elementtypen und der genannten Werte an einen speziellen Elementtyp und -wert; und

   Interpretieren der genannten Platzhalterkennungen.

9. Eine Methode nach jedem der vorangegangenen Ansprüche, weiterhin folgende Schritte umfassend:

   Akzeptieren eines vom Benutzer erstellten Einwirkungsassoziations-Schemas als Eingabe, wobei das genannte Einwirkungsassoziations-Schema zur Konstruktion einer Einwirkungstabelle verwendet wird;

   Erhalten einer Ereignisgruppe als Eingabe;

   Anwenden der genannten Ereignisgruppe auf die genannte Einwirkungstabelle zur Bestimmung der genannten speziellen Einwirkungen, wobei die genannten speziellen Einwirkungen durch einen Vergleich der Eigenschaften der genannten Ereignisgruppe mit den in der genannten Einwirkungstabelle enthaltenen Daten bestimmt werden; und

   Ausgeben der genannten speziellen Einwirkungen an ein Anwendungsprogramm zur weiteren Verarbeitung.

10. Eine Methode nach Anspruch 9, bei der genannte Schritt der Ausgabe weiterhin folgenden Schritt umfaßt:

   Senden der genannten speziellen Einwirkungen an eine Person mit einer elektronischen Adresse in einem Computersystem.

11. Eine Methode nach Anspruch 9, bei der die genannte Einwirkungstabellen-Konstruktion weiterhin folgende Schritte umfaßt:

   Akzeptieren der Benutzereingabe zur Erstellung und Änderung des genannten Einwirkungsassoziations-Schemas; und

   Syntaktisches Analysieren der genannten Benutzereingabe in einer gerätespezifischen Darstellung.

12. Eine Methode nach Anspruch 11, bei der die genannte Einwirkullgstabellen-Konstruktion weiterhin folgenden Schritt umfaßt:

Aufnahme einer Vielzahl von Gruppeneingaben in eine Einwirkungstabelle.

13. Eine Methode nach Anspruch 12, bei der der genannte Schritt der Aufnahme von Gruppeneingaben weiterhin folgenden Schritt umfaßt:

Hinzufügen einer Gruppenkennung und Einwirkungen zu den genannten Gruppeneingaben.

14. Eine Methode nach Anspruch 13, bei der der genannte Schritt der Einwirkungsbestimmung weiterhin folgende Schritte umfaßt:

Verwenden der genannten Gruppenkennung zum Durchsuchen der genannten Gruppeneingaben; und

Anpassen der genannten Gruppenkennung an einen speziellen Gruppentyp.

15. Eine Vorrichtung zur Ereignisbehandlung in einem Ereignisstrom (25) eines Datenverarbeitungssystems, wobei die genannte Vorrichtung weiterhin folgendes umfaßt:

Ein Mittel zum Akzeptieren eines vom Benutzer erstellten Kategorisierungsschemas als Eingabe, das zur Konstruktion einer Filtertabelle (32) verwendet wird, die als Eingabe die genannten Ereignisse erhält;

Ein Mittel zum Anwenden der genannten Ereignisse auf die genannte Filtertabelle; und

Ein Mittel zum Kategorisieren der genannten Ereignisse in Ereignisgruppen, basierend auf einem Vergleich der Eigenschaften der genannten Ereignisse mit den in der genannten Filtertabelle (32) enthaltenen Daten.

16. Eine Vorrichtung nach Anspruch 15, bei der die genannten Mittel zum Akzeptieren des genannten vom Benutzer erstellten Kategorisierungsschemas weiterhin folgendes umfassen:

Ein Mittel zum Akzeptieren von Benutzereingaben zur Konstruktion und Änderung des genannten Kategorisierungsschemas.

17. Eine Vorrichtung nach Anspruch 16, bei der die genannten Mittel zum Akzeptieren der Benutzereingabe weiterhin folgendes umfassen:

Ein Mittel zum syntaktischen Analysieren der genannten Benutzereingabe in einer gerätespezifischen Darstellung.

18. Eine Vorrichtung nach Anspruch 17, bei der die genannte Filtertabelle eine Vielzahl an sequentiell angeordneten Filtereingaben (33) enthält, wobei jede der genannten Filtereingaben eine Gruppenkennung, eine Sequenznummer und einen Satz an Auswahlkriterien umfaßt.

19. Eine Vorrichtung nach Anspruch 18, bei der der genannte Satz an Auswahlkriterien einen Satz an Elementtypen, Orten und Operatoren umfaßt, wobei die genannten Operatoren relational sind.

20. Eine Vorrichtung nach Anspruch 19, bei der die genannten Operatoren Boolesche Operatoren sind.

21. Eine Vorrichtung nach Anspruch 20, bei der der genannte Wert eine Platzhalterkennung umfaßt.

22. Eine Vorrichtung nach Anspruch 15, bei der die genannten Mittel zum Akzeptieren von Benutzereingaben weiterhin folgendes umfassen:

Ein Mittel zum syntaktischen Analysieren der genannten Ereignisse in standardisierte Ereignisse.

23. Eine Vorrichtung nach Anspruch 21, bei der die genannten Mittel zum Anwenden weiterhin folgendes umfassen:

Ein Mittel zum Verwenden der genannten Sequenznummern zum Durchsuchen der genannten Filtereingaben;

Ein Mittel zum Anpassen der genannten Elementtypen und der genannten Werte an einen speziellen Elementtyp und -wert; und

Ein Mittel zum Interpretieren der genannten Platzhalterkennungen.

24. Eine Vorrichtung nach den Ansprüchen 15 bis 23, weiterhin folgendes umfassend:

in Mittel zum Akzeptieren eines vom Benutzer erstellten Einwirkungsassoziations-Schemas, wobei das genannte Einwirkungsassoziations-Schema zur Konstruktion einer Einwirkungstabelle (37) verwendet wird;

Ein Mittel zum Erhalten einer Ereignisgruppe als Eingabe;

Ein Mittel zum Anwenden der genannten Ereignisgruppe auf die genannte Einwirkungstabelle, um die genannten speziellen Einwirkungen festzulegen, wobei die genannten speziellen Einwirkungen durch einen Vergleich der Eigenschaften der genannten Ereignisgruppe mit den in der genannten Einwirkungstabelle enthaltenen Daten bestimmt werden; und

Ein Mittel zum Ausgeben der genannten speziellen Einwirkungen an ein Anwendungsprogramm zur weiteren Verarbeitung.

25. Eine Vorrichtung nach Anspruch 24, bei der das Ziel der genannten Mittel zur Ausgabe eine Person mit einer elektronischen Adresse in einem Computersystem ist.

26. Eine Vorrichtung nach Anspruch 24, bei der die genannte Einwirkungstabellen-Konstruktion weiterhin folgende Mittel umfaßt:

Ein Mittel zum Akzeptieren von Benutzereingaben zur Erstellung und Änderung des genannten Einwirkungsassoziations-Schemas; und

Ein Mittel zum syntaktischen Analysieren der genannten Benutzereingabe in einer gerätespezifischen Darstellung.

27. Eine Vorrichtung nach Anspruch 26, bei der das genannte Mittel zur Einwirkungstabellen-Konstruktion weiterhin folgendes Mittel umfaßt:

Ein Mittel zum Aufnehmen einer Vielzahl von Gruppeneinträgen in eine Einwirkungstabelle.

28. Eine Vorrichtung nach Anspruch 27, bei der das genannte Mittel zum Aufnehmen von Gruppeneinträgen weiterhin folgendes Mittel umfaßt:

Ein Mittel zum Hinzufügen einer Gruppenkennung und Einwirkungen zu den einzelnen genannten Gruppeneinträgen.

29. Eine Vorrichtung nach Anspruch 28, bei der die genannten Mittel zum Bestimmen der speziellen Einwirkungen weiterhin folgendes Mittel umfassen:

Ein Mittel zum Verwenden der genannten Gruppenkennungen zum Durchsuchen der genannten Gruppeneinträge; und

Ein Mittel zum Anpassen der genannten Gruppenkennungen an eine spezielle Gruppe.

Revendications

1. Un procédé de traitement d'événements dans un flux d'événements (25) d'un système de traitement de données, ledit procédé comprenant les étapes consistant à :

accepter comme entrée un schéma de catégorisation ayant été créé par l'utilisateur, ledit schéma de catégorisation créé par l'utilisateur étant utilisé pour construire une table de filtre (32) recevant comme entrée lesdits événements;

appliquer lesdits événements à ladite table de filtre; et

classer en catégorie lesdits événements, en groupes événements, en se basant sur une comparaison de caractéristiques desdits événements, avec l'information contenue dans ladite table de filtre.

2. Le procédé selon la revendication 1, dans lequel ladite étape d'acceptation dudit schéma de classement en catégorie par l'utilisateur comprend en outre les étapes consistant à :

accepter comme entrée un schéma de catégorisation utilisateur modifié pas ; et

effectuer une analyse de ladite entrée utilisateur, dans une représentation spécifique au dispositif.

3. Le procédé selon la revendication 2, dans lequel ladite étape d'acceptation comprend en outre l'étape consistant à :

introduire une pluralité d'entrées de filtre (33) agencés séquentiellement dans ladite table de filtre (32).

4. Le procédé selon la revendication 3, dans lequel ladite table d'entrée comprend en outre l'étape consistant à :

ajouter un identificateur de groupe, un numéro de séquence, et un jeu de critères de sélection à chacune desdites entrées de filtre.

5. Le procédé selon la revendication 4, dans lequel ladite étape d'addition comprend en outre l'étape consistant à :

introduire comme partie dudit critère de sélection un jeu de types d'élément, de valeurs et d'opérateurs.

6. Le procédé selon la revendication 5, dans lequel ladite étape d'introduction comprenant en outre l'étape consistant à :

placer un identificateur de caractère joker dans ladite valeur.

7. Le procédé selon la revendication 1, dans lequel ladite étape d'application comprend en outre l'étape consistant à effectuer une analyse desdits événements en événements standardisés.

8. Le procédé selon la revendication 6, dans lequel ladite étape de catégorisation comprend en outre une étape consistant à :

   utiliser lesdits numéraux de séquence pour faire une recherche dans lesdites entrées de filtre;

   adapter lesdits types d'élément et lesdites valeurs à un type et à une valeur d'élément particuliers; et

   interpréter lesdits identificateurs de caractère joker.

9. Le procédé selon l'une quelconque des revendications précédentes comprenant en outre les étapes consistant à :

   accepter comme entrée un schéma d'association d'action créé par l'utilisateur, ledit schéma d'association d'action étant utilisé pour construire une table d'action (37);

   recevoir comme entrée un groupe événements;

   appliquer ledit groupe événements à ladite table d'action pour déterminer lesdites actions particulières, lesdites actions particulières étant déterminées par une comparaison des caractéristiques dudit groupe événements avec une information contenue dans ladite table d'action; et

   envoyer lesdites actions particulières à un programme d'application pour continuer le traitement.

10. Le procédé selon la revendication 9, dans lequel ladite étape d'envoi comprend en outre :

   l'envoi desdites actions particulières à une personne située à une adresse électronique sur un système d'ordinateur.

11. Le procédé selon la revendication 9, dans lequel ladite étape de construction étape d'action comprend en outre les étapes consistant à :

   accepter une entrée utilisateur pour créer et modifier ledit schéma d'association d'action; et

   effectuer une analyse sur l'entrée utilisateur, en une représentation spécifique au dispositif.

12. Le procédé selon la revendication 11, dans lequel ladite étape de construction de table d'action comprend en outre l'étape consistant à :

   introduire une pluralité d'entrées de groupe dans une table d'action.

13. Le procédé selon la revendication 12, dans lequel ladite étape d'introduction d'entrée de groupe comprend en outre l'étape consistant à :

   ajouter un identificateur de groupe et des actions à chacune desdites entrées de groupe.

14. Le procédé selon la revendication 13, dans lequel ladite étape de détermination d'action comprend en outre les étapes consistant à :

   utiliser lesdits identificateurs de groupe pour rechercher dans lesdites entrées de groupe; et

   adapter ledit identificateur de groupe à un type de groupe particulier.

15. Un dispositif de traitement événements dans un flot de données (25) d'un système de traitement de données, ledit appareil comprenant :

   des moyens pour accepter comme entrée un schéma de catégorisation crée par l'utilisateur, ledit schéma de catégorisation crée par l'utilisateur étant utilisé pour construire une table de filtre (32) recevant comme entrée lesdits événements;

   des moyens pour appliquer lesdits événements à ladite table de filtre; et

   des moyens pour catégoriser lesdits événements en des groupes événements, en se basant sur une comparaison des caractéristiques desdits événements avec l'information contenue dans ladite table de filtre (32).

16. Le dispositif selon la revendication 15, dans lequel lesdits moyens d'acceptation dudit schéma de catégorisation utilisateur comprennent en outre :

   des moyens pour accepter l'entrée utilisateur pour construire et modifier ledit schéma de catégorisation.

17. Le dispositif selon la revendication 16, dans lequel lesdits moyens d'acceptation de l'entrée utilisateur comprennent en outre :

des moyens pour effectuer une analyse sur ladite entrée utilisateur, en une représentation spécifique au dispositif.

18. Le dispositif selon la revendication 17, dans lequel ladite étape de filtre comprend une pluralité d'entrée de filtre (33) agencées séquentiellement, chacune desdites entrées de filtre comprenant un identificateur de groupe, un numéro de séquence, et un jeu de critères de sélection.

19. Le dispositif selon la revendication 18, dans lequel ledit jeu de critères de sélection comprend un jeu de types d'élément, de valeurs, et d'opérateurs, lesdits opérateurs étant de type relationnel.

20. Le dispositif selon la revendication 19, dans lequel lesdits opérateurs sont Booléens.

21. Le dispositif selon la revendication 20, dans lequel ladite valeur comprend un identificateur de caractère joker.

22. Le dispositif selon la revendication 15, dans lequel lesdits moyens d'acceptation de l'entrée utilisateur comprennent en outre :

des moyens pour effectuer une analyse desdits événements en des éléments standardisés.

23. Le dispositif selon la revendication 21, dans lequel lesdits moyens d'application comprennent en outre :

des moyens pour utiliser lesdits numéros de séquence pour faire une recherche dans lesdites entrées de filtre;

des moyens pour adapter lesdits types d'élément et lesdites valeurs à un type et à une valeur particuliers d'élément;

des moyens pour interpréter lesdits identificateurs de caractère joker.

24. Le dispositif selon l'une quelconque des revendications 15 à 23, comprenant en outre :

des moyens pour accepter comme entrée un schéma d'association d'action crée par l'utilisateur, ledit schéma d'association d'action étant utilisé pour construire une table d'action (37);

des moyens pour recevoir comme entrée un groupe d'événements;

des moyens pour appliquer ledit groupe d'événements à ladite table d'action pour déterminer lesdites actions particulières, lesdites actions particulières étant déterminées par comparaison des caractéristiques dudit groupe d'événements avec une information contenue dans ladite table d'action;

des moyens pour envoyer lesdites actions particulières à un programme d'application pour continuer le traitement.

25. Le dispositif selon la revendication 24, dans lequel une destination desdits moyens pour envoi est une personne placée à une adresse électronique sur un système d'ordinateur.

26. Le dispositif selon la revendication 24, dans lequel lesdits moyens de construction de table d'action comprennent en outre des moyens pour :

accepter l'entrée utilisateur pour créer et modifier ledit schéma d'association d'action; et

effectuer une analyse sur ladite entrée utilisateur en une représentation spécifique au dispositif.

27. Le dispositif selon la revendication 26, dans lequel lesdits moyens de construction de table d'action comprennent en outre des moyens pour :

envoyer une pluralité d'entrées de groupe dans une table d'action.

28. Le dispositif selon la revendication 27, dans lequel lesdits moyens d'introduction d'entrées de groupe comprennent en outre des moyens pour :

ajouter un identificateur de groupe et des actions à chacune desdites entrées de groupe.

29. Le dispositif selon la revendication 28, dans lequel lesdits moyens de détermination desdites actions particulières comprennent en outre des moyens pour :

utiliser lesdits identificateurs de groupe pour effectuer une recherche dans lesdites entrées de groupe; et

adapter ledit identificateur de groupe à un groupe particulier.

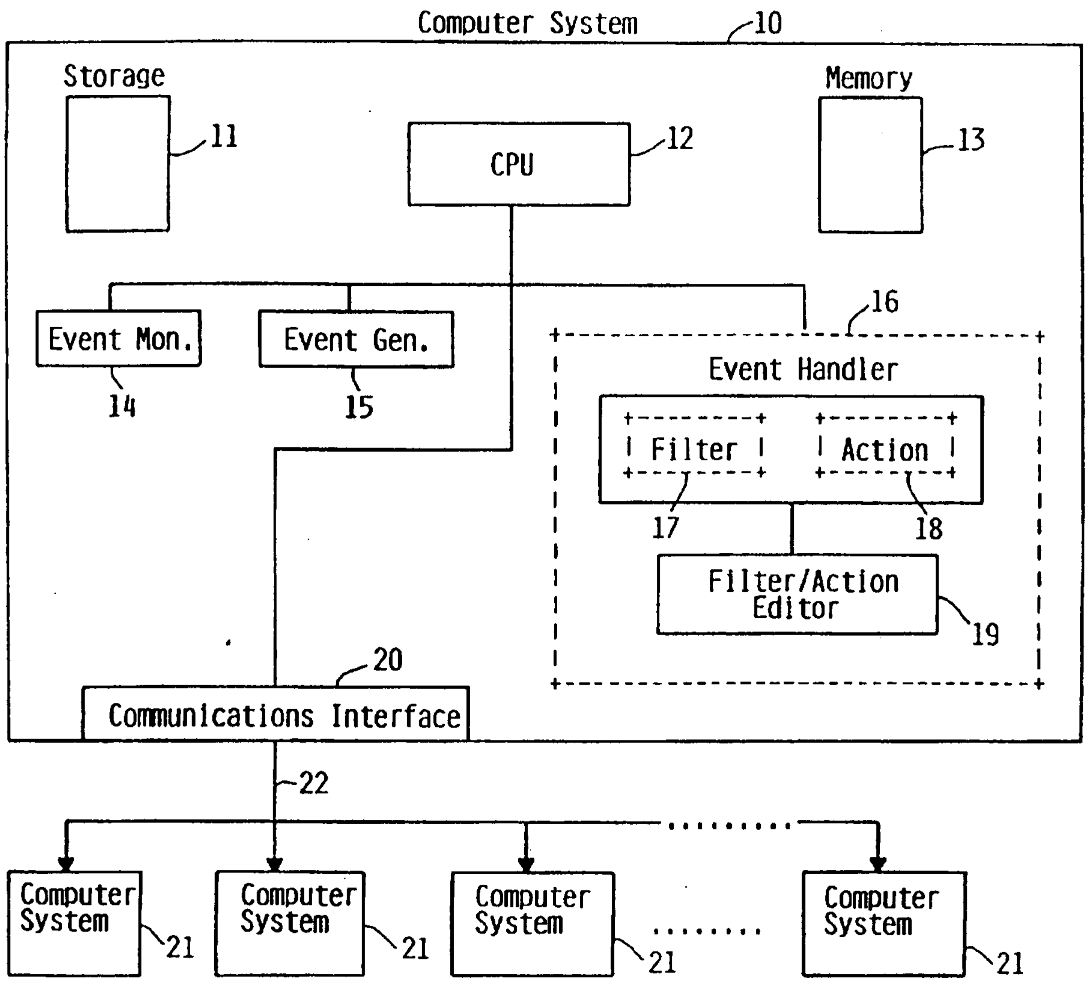

Computer System
10
Storage
11
CPU
12
Memory
13
Event Mon.
14
Event Gen.
15
16
Event Handler
Filter
Action
17
18
Filter/Action Editor
19
20
Communications Interface
22
Computer System
21
Computer System
21
Computer System
21
Computer System
21

FIG. I

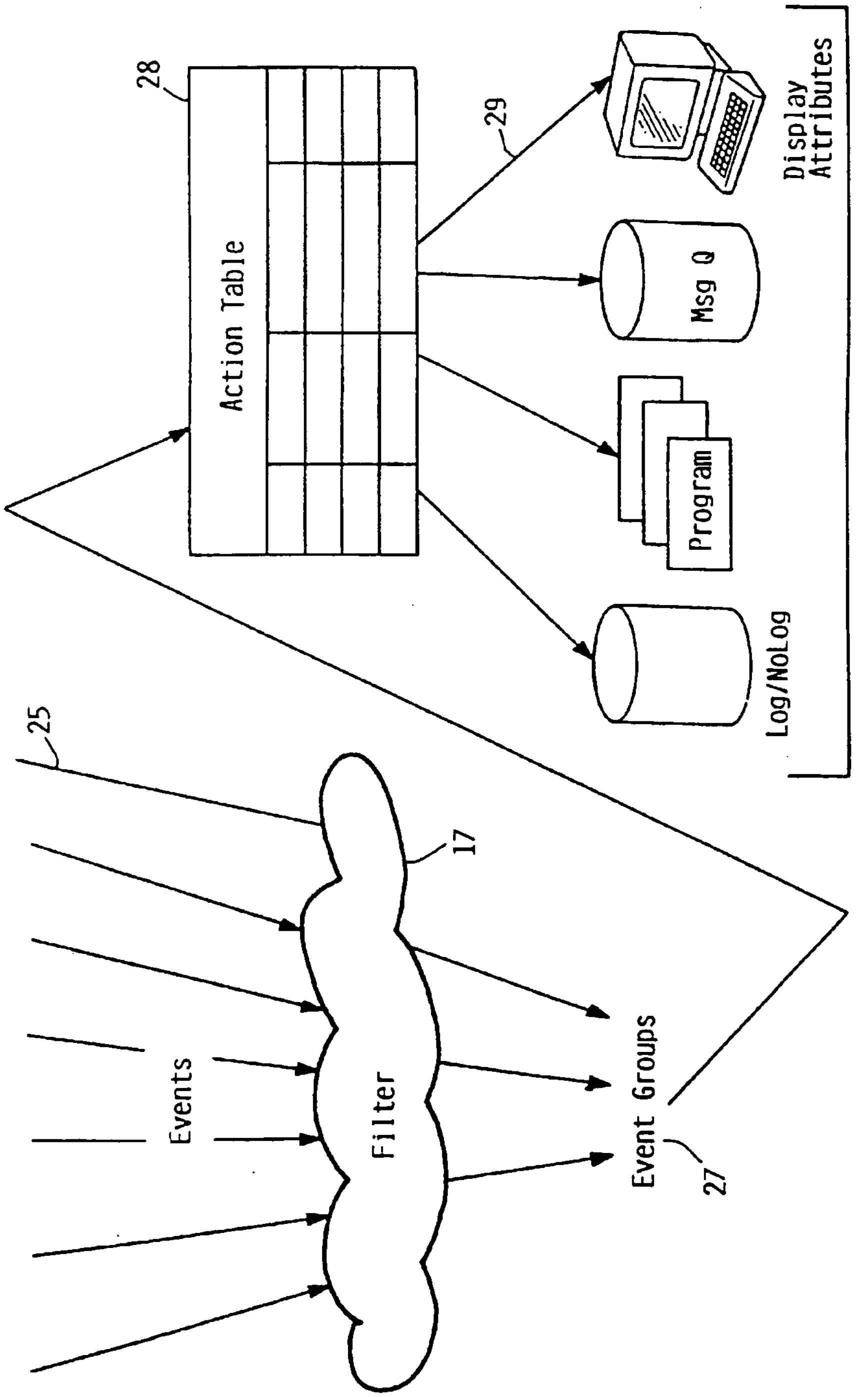

28
Action Table
29
Display Attributes
Msg Q
Program
Log/NoLog
Actions
25
17
Events
Filter
Event Groups
27

FIG. 2

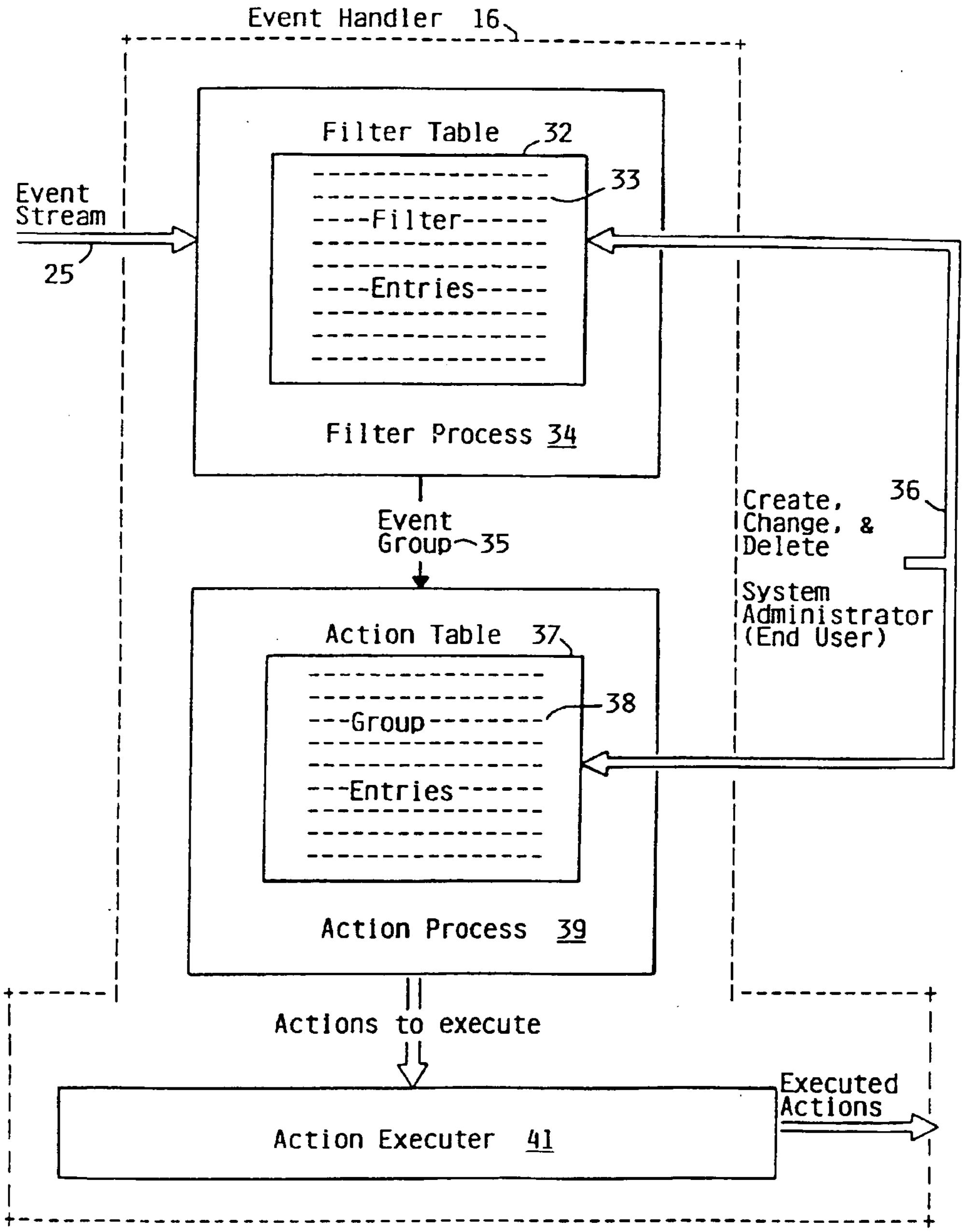

Event Handler 16
Filter Table 32
33
----Filter------
----Entries-----
Filter Process 34
Event Stream
25
Event Group 35
Create, Change, & Delete
36
System Administrator (End User)
Action Table 37
38
---Group--------
---Entries------
Action Process 39
Actions to execute
Action Executer 41
Executed Actions

FIG. 3

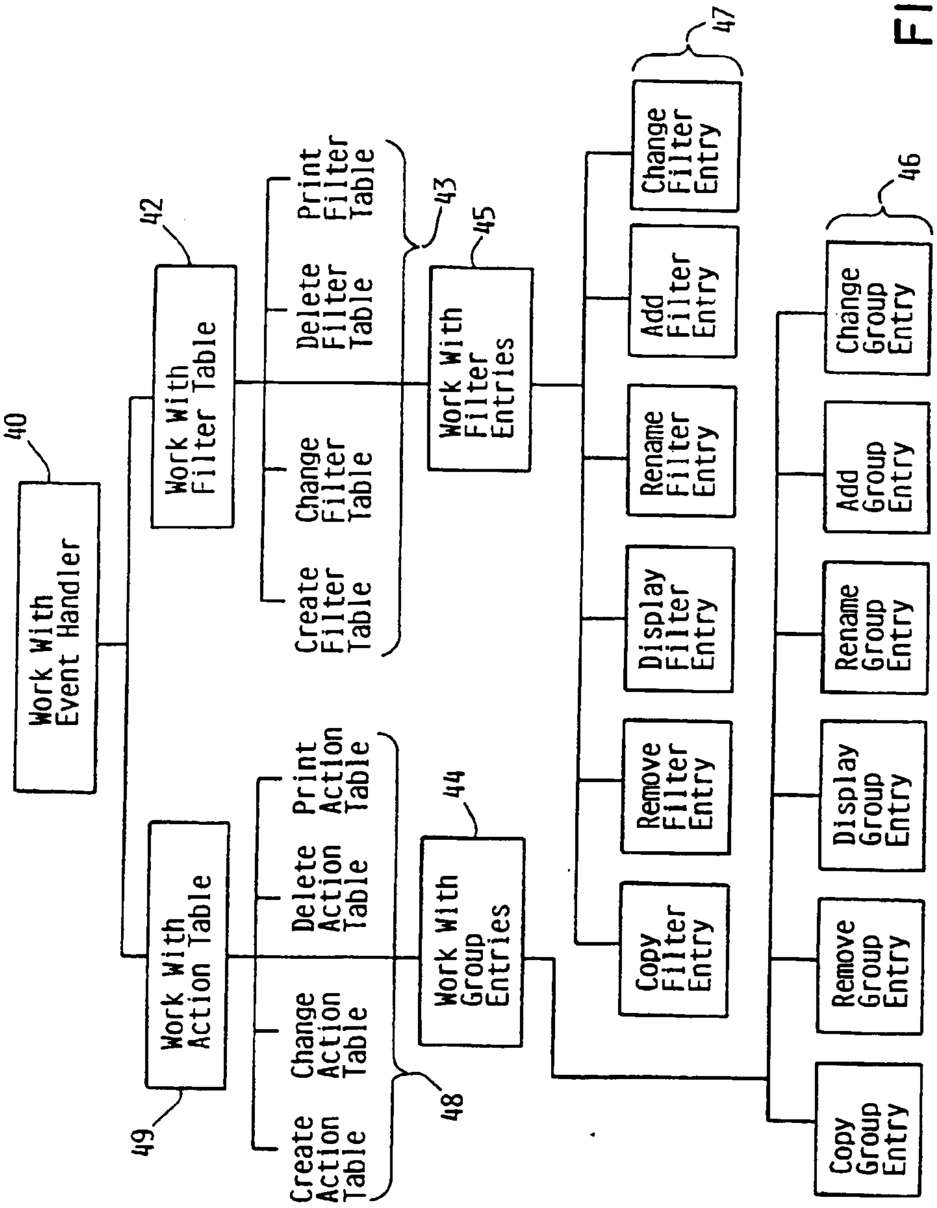
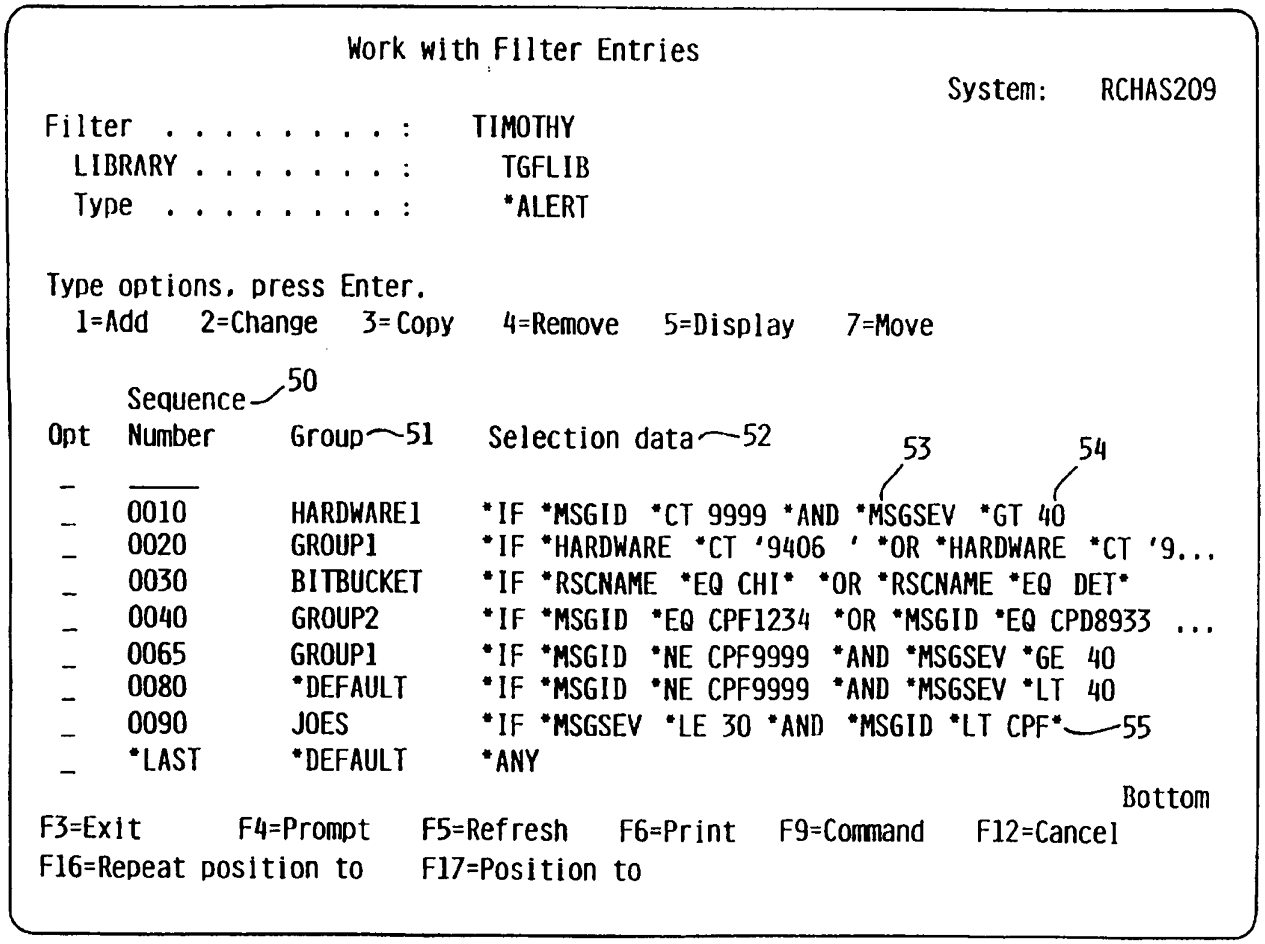

40
Work With Event Handler
42
Work With Filter Table
Create Filter Table
Change Filter Table
Delete Filter Table
Print Filter Table
43
45
Work With Filter Entries
Copy Filter Entry
Remove Filter Entry
Display Filter Entry
Rename Filter Entry
Add Filter Entry
Change Filter Entry
47
49
Work With Action Table
Create Action Table
Change Action Table
Delete Action Table
Print Action Table
48
44
Work With Group Entries
Copy Group Entry
Remove Group Entry
Display Group Entry
Rename Group Entry
Add Group Entry
Change Group Entry
46

FIG. 4



```
                    Work with Filter Entries
                                                          System:    RCHAS209
Filter . . . . . . . . . :      TIMOTHY
  LIBRARY . . . . . . . . :       TGFLIB
  Type  . . . . . . . . . :       *ALERT

Type options, press Enter.
  1=Add    2=Change    3=Copy    4=Remove    5=Display    7=Move

     Sequence
Opt  Number       Group        Selection data

 _   ____
 _   0010         HARDWARE1    *IF *MSGID  *CT 9999 *AND *MSGSEV  *GT 40
 _   0020         GROUP1       *IF *HARDWARE  *CT '9406 ' *OR *HARDWARE  *CT '9...
 _   0030         BITBUCKET    *IF *RSCNAME  *EQ CHI*  *OR *RSCNAME *EQ  DET*
 _   0040         GROUP2       *IF *MSGID  *EQ CPF1234  *OR *MSGID *EQ CPD8933  ...
 _   0065         GROUP1       *IF *MSGID  *NE CPF9999  *AND *MSGSEV *GE  40
 _   0080         *DEFAULT     *IF *MSGID  *NE CPF9999  *AND *MSGSEV *LT  40
 _   0090         JOES         *IF *MSGSEV  *LE 30 *AND  *MSGID *LT CPF*
 _   *LAST        *DEFAULT     *ANY
                                                                      Bottom
F3=Exit       F4=Prompt    F5=Refresh    F6=Print    F9=Command    F12=Cancel
F16=Repeat position to     F17=Position to
```

FIG. 5

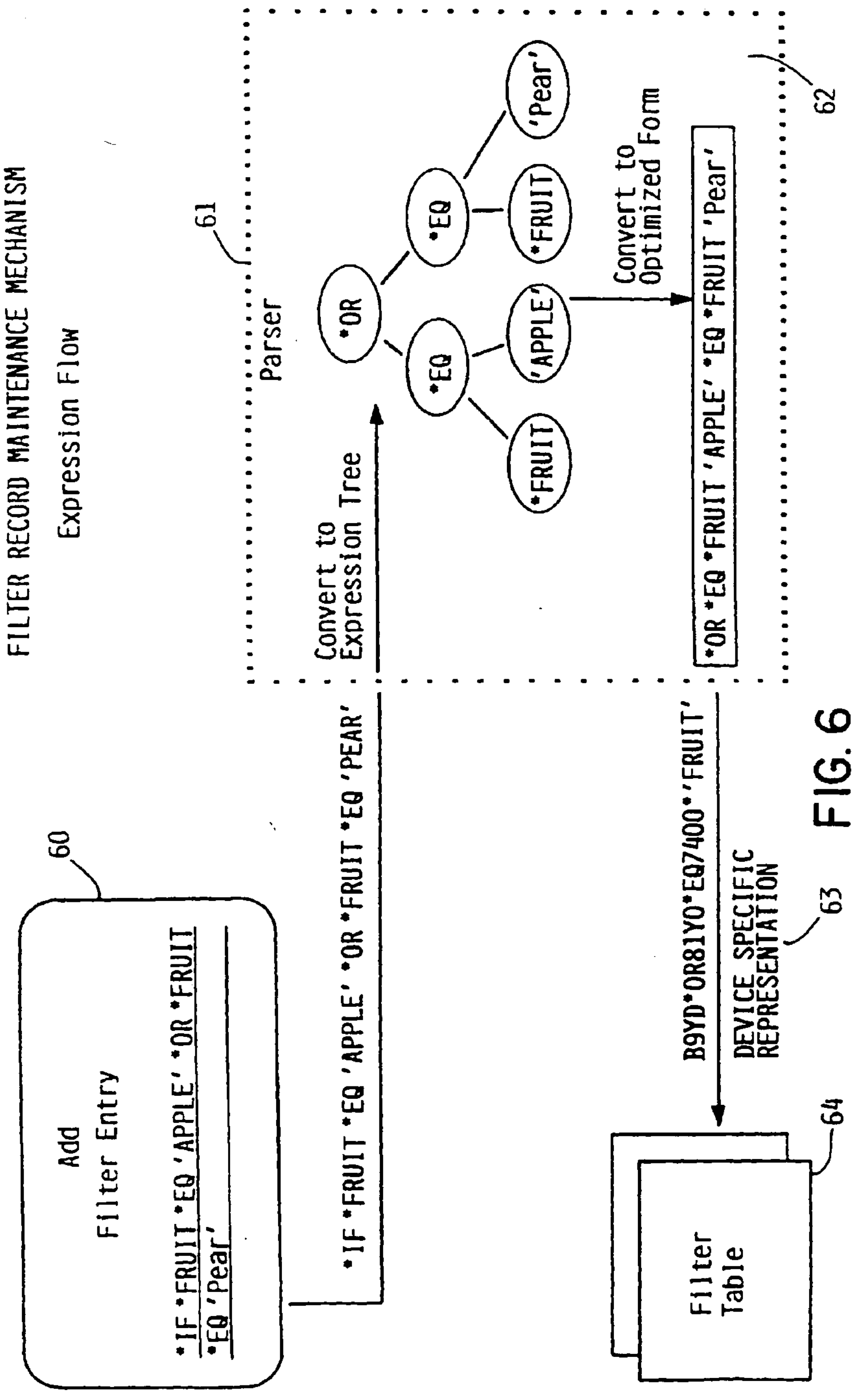
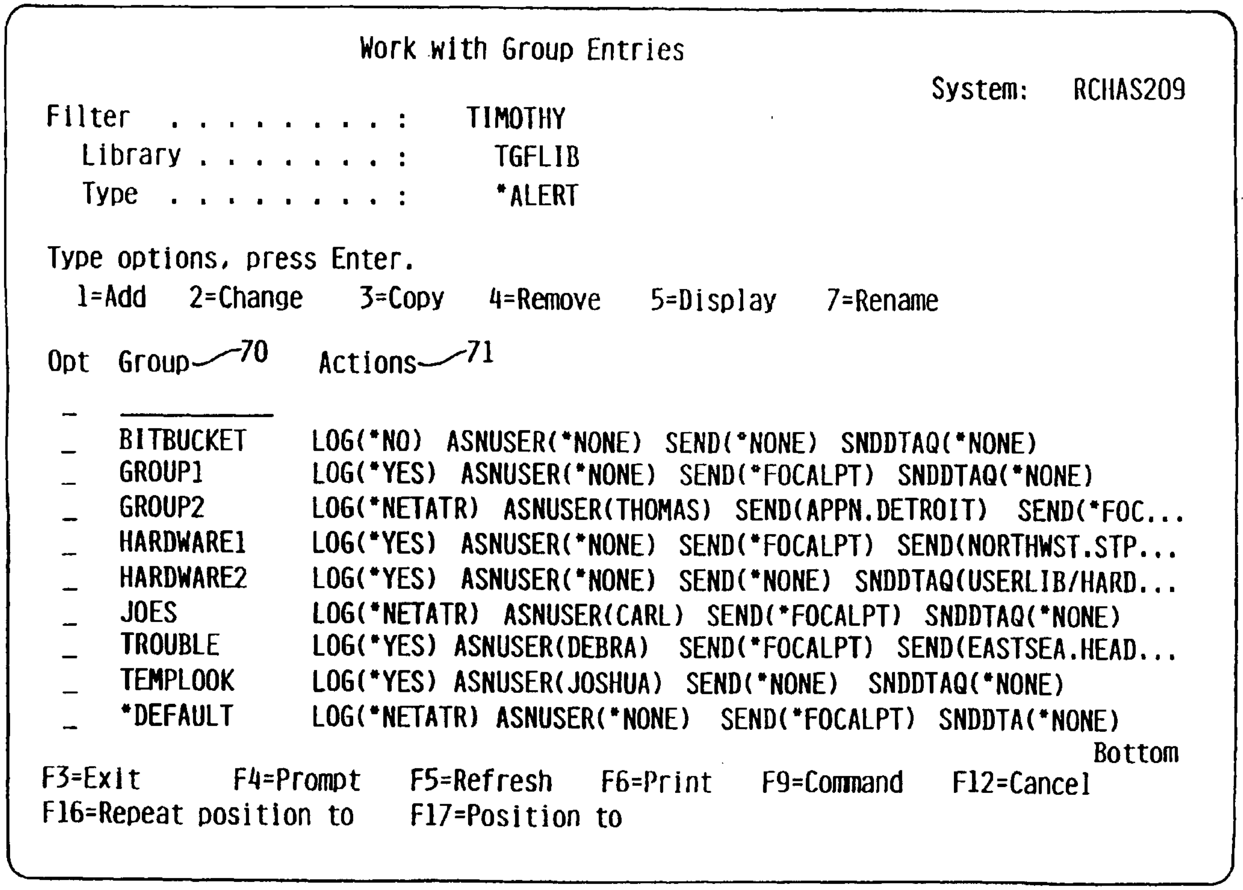

FILTER RECORD MAINTENANCE MECHANISM
Expression Flow
60
Add
Filter Entry
*IF *FRUIT *EQ 'APPLE' *OR *FRUIT *EQ 'Pear'
*IF *FRUIT *EQ 'APPLE' *OR *FRUIT *EQ 'PEAR'
Convert to Expression Tree
61
Parser
*OR
*EQ
*EQ
*FRUIT
'APPLE'
*FRUIT
'Pear'
Convert to Optimized Form
*OR *EQ *FRUIT 'APPLE' *EQ *FRUIT 'Pear'
62
B9YD*OR81YO*EQ7400*'FRUIT'
DEVICE SPECIFIC REPRESENTATION
63
64
Filter
Table

FIG. 6



```
                    Work with Group Entries
                                                   System:   RCHAS209
Filter . . . . . . . . . :    TIMOTHY
  Library . . . . . . . . :     TGFLIB
  Type  . . . . . . . . . :     *ALERT

Type options, press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display   7=Rename

Opt  Group      Actions

 _
 _   BITBUCKET  LOG(*NO)  ASNUSER(*NONE)  SEND(*NONE)  SNDDTAQ(*NONE)
 _   GROUP1     LOG(*YES)  ASNUSER(*NONE)  SEND(*FOCALPT)  SNDDTAQ(*NONE)
 _   GROUP2     LOG(*NETATR)  ASNUSER(THOMAS)  SEND(APPN.DETROIT)  SEND(*FOC...
 _   HARDWARE1  LOG(*YES)  ASNUSER(*NONE)  SEND(*FOCALPT)  SEND(NORTHWST.STP...
 _   HARDWARE2  LOG(*YES)  ASNUSER(*NONE)  SEND(*NONE)  SNDDTAQ(USERLIB/HARD...
 _   JOES       LOG(*NETATR)  ASNUSER(CARL)  SEND(*FOCALPT)  SNDDTAQ(*NONE)
 _   TROUBLE    LOG(*YES) ASNUSER(DEBRA)  SEND(*FOCALPT)  SEND(EASTSEA.HEAD...
 _   TEMPLOOK   LOG(*YES) ASNUSER(JOSHUA)  SEND(*NONE)  SNDDTAQ(*NONE)
 _   *DEFAULT   LOG(*NETATR) ASNUSER(*NONE)  SEND(*FOCALPT)  SNDDTA(*NONE)
                                                                   Bottom
F3=Exit     F4=Prompt   F5=Refresh   F6=Print   F9=Command   F12=Cancel
F16=Repeat position to  F17=Position to
```

FIG. 7

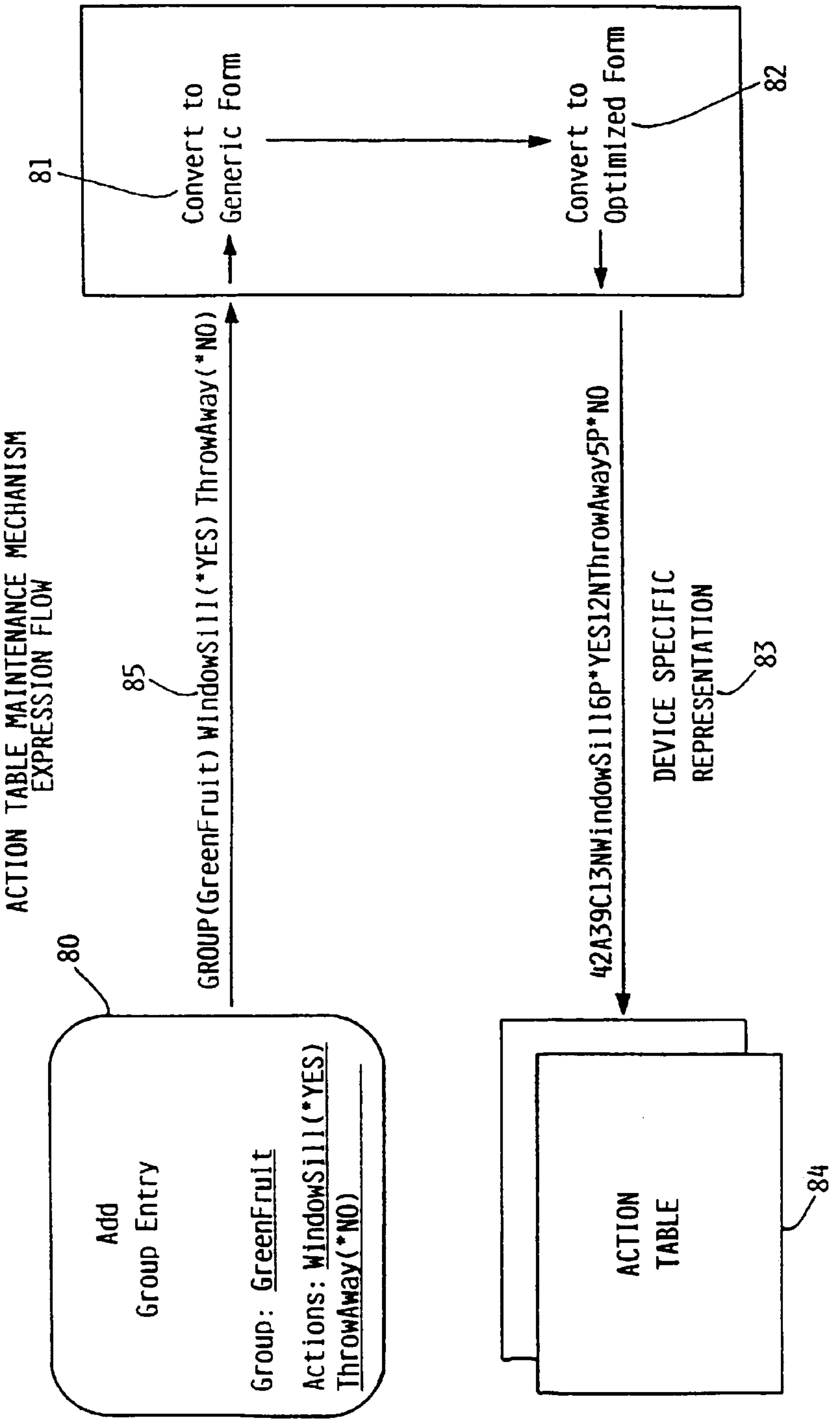

ACTION TABLE MAINTENANCE MECHANISM
EXPRESSION FLOW
80
Add
Group Entry
Group: GreenFruit
Actions: WindowSill(*YES)
ThrowAway(*NO)
85
GROUP(GreenFruit) WindowSill(*YES) ThrowAway(*NO)
81
Convert to
Generic Form
Convert to
Optimized Form
82
42A39C13NWindowSill6P*YES12NThrowAway5P*NO
DEVICE SPECIFIC
REPRESENTATION
83
ACTION
TABLE
84

FIG. 8

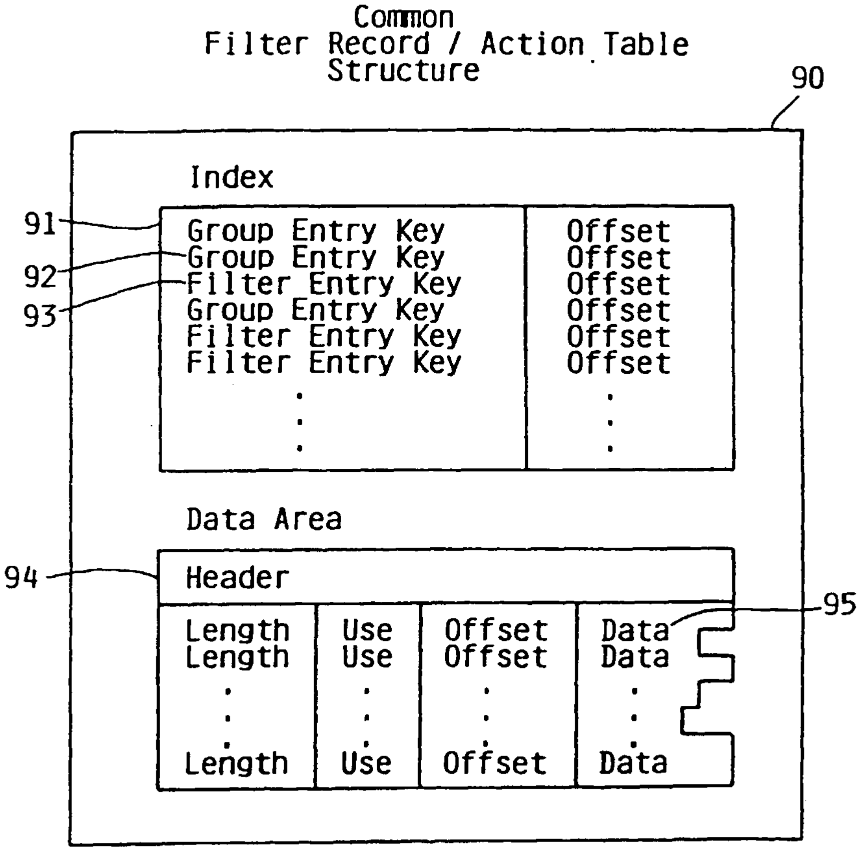

Common
Filter Record / Action Table
Structure
90
Index
91
92
93
Group Entry Key
Group Entry Key
Filter Entry Key
Group Entry Key
Filter Entry Key
Filter Entry Key
Offset
Offset
Offset
Offset
Offset
Offset
Data Area
94
Header
95
Length
Length
Length
Use
Use
Use
Offset
Offset
Offset
Data
Data
Data

FIG. 9

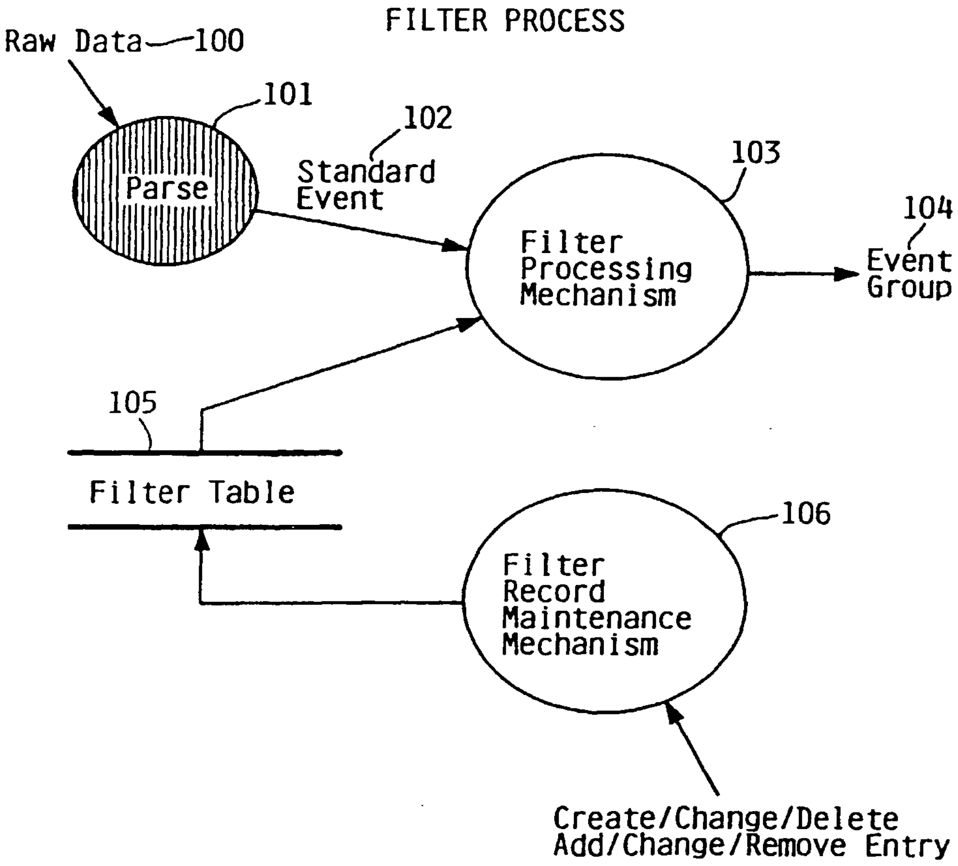
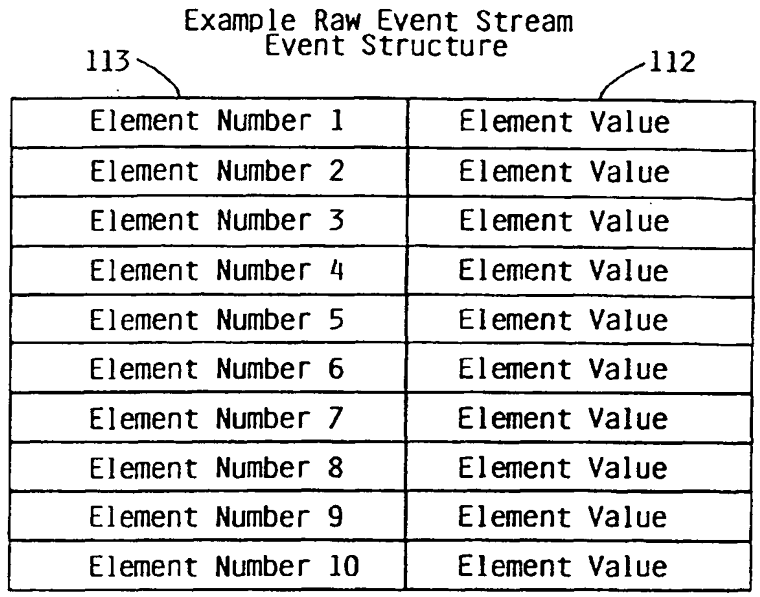

FILTER PROCESS
Raw Data
100
101
Parse
102
Standard Event
103
Filter Processing Mechanism
104
Event Group
105
Filter Table
106
Filter Record Maintenance Mechanism
Create/Change/Delete
Add/Change/Remove Entry

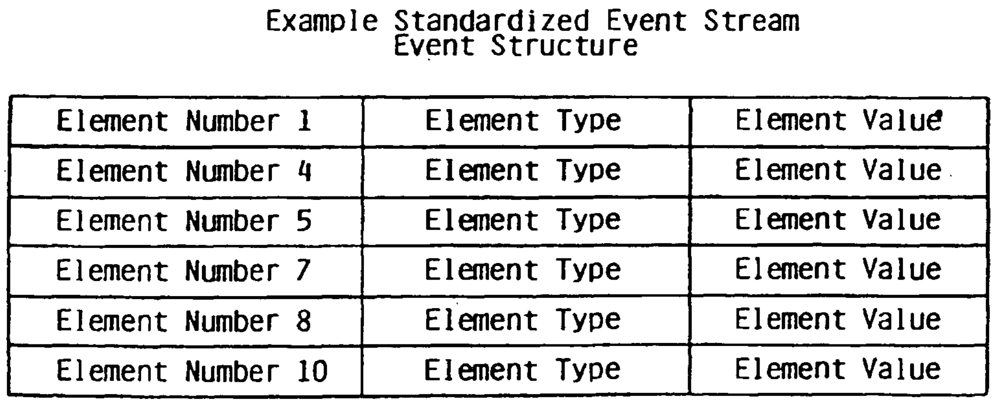
FIG. 10



Example Raw Event Stream
Event Structure

Element Number 1	Element Value
Element Number 2	Element Value
Element Number 3	Element Value
Element Number 4	Element Value
Element Number 5	Element Value
Element Number 6	Element Value
Element Number 7	Element Value
Element Number 8	Element Value
Element Number 9	Element Value
Element Number 10	Element Value

FIG. 11



Example Standardized Event Stream
Event Structure

Element Number 1	Element Type	Element Value
Element Number 4	Element Type	Element Value
Element Number 5	Element Type	Element Value
Element Number 7	Element Type	Element Value
Element Number 8	Element Type	Element Value
Element Number 10	Element Type	Element Value

FIG. 12

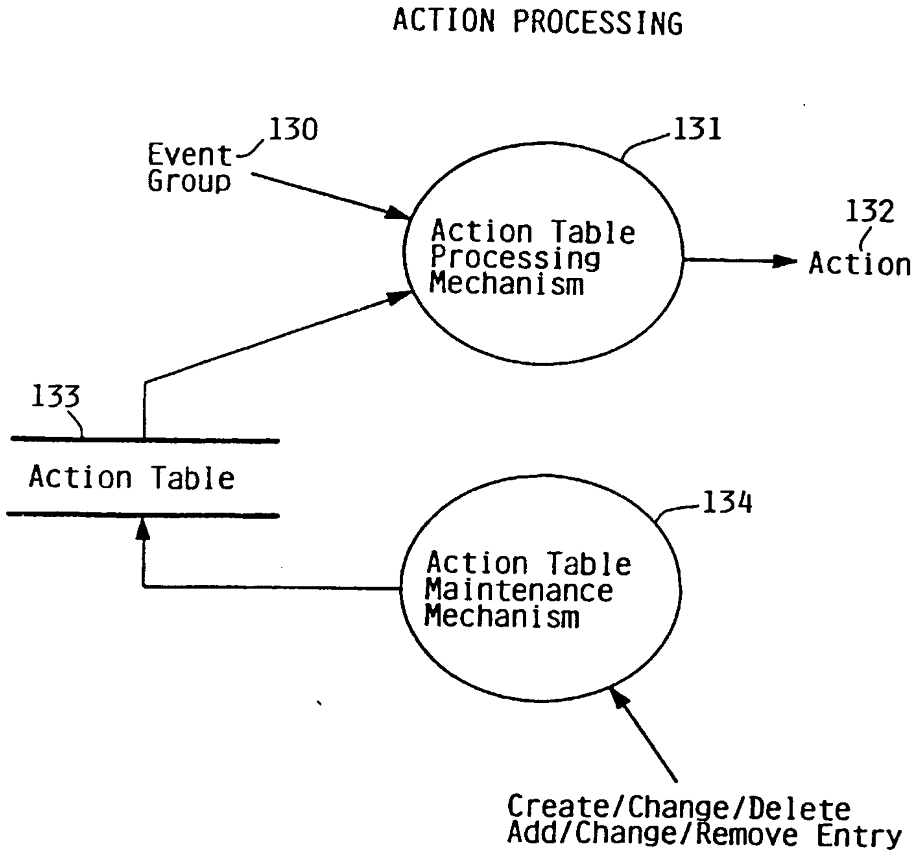

ACTION PROCESSING
130
Event Group
131
Action Table Processing Mechanism
132
Action
133
Action Table
134
Action Table Maintenance Mechanism
Create/Change/Delete
Add/Change/Remove Entry

FIG. 13

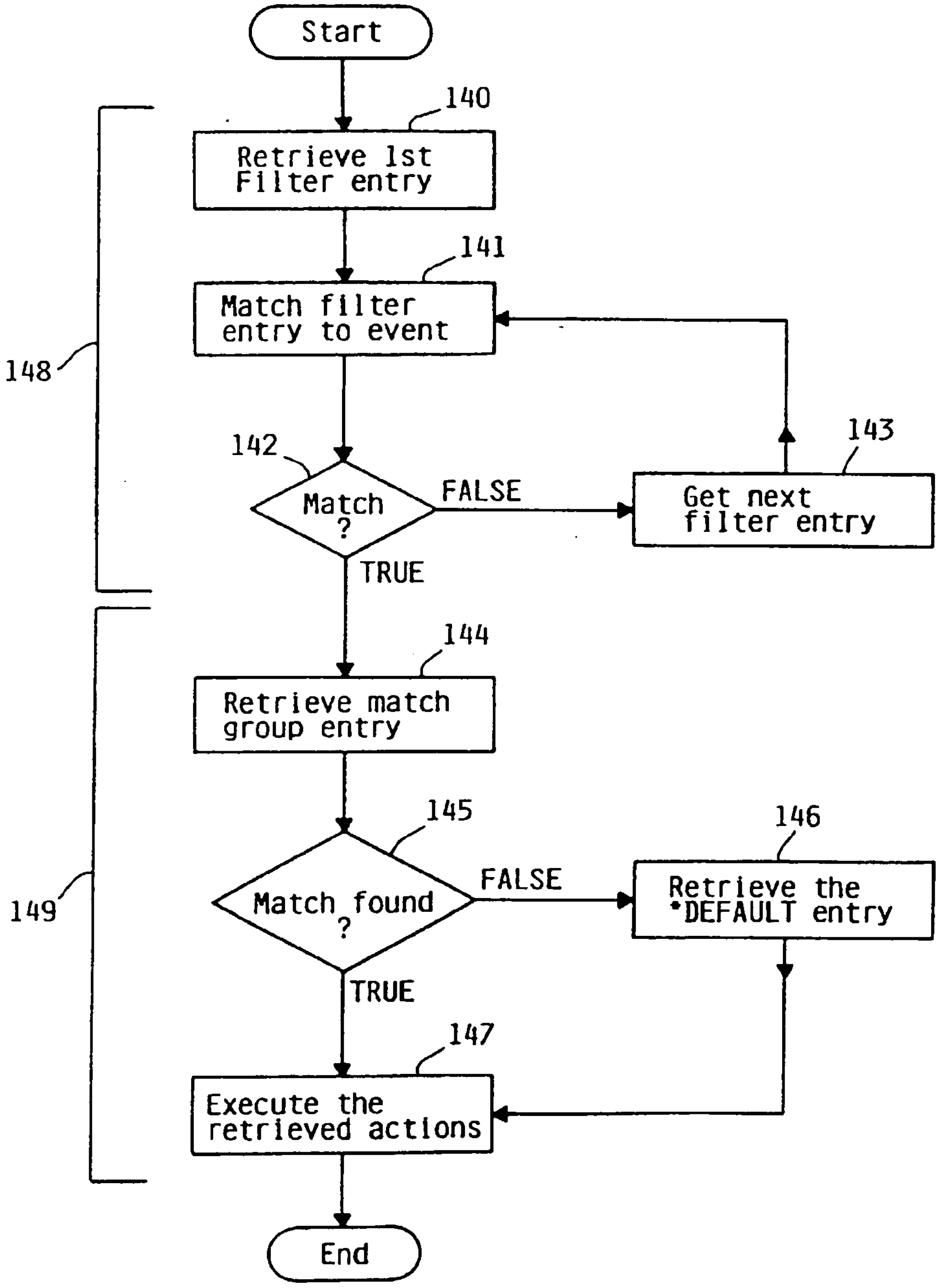

Start
140
Retrieve 1st Filter entry
141
Match filter entry to event
148
142
Match ?
FALSE
TRUE
143
Get next filter entry
144
Retrieve match group entry
145
Match found ?
FALSE
TRUE
146
Retrieve the *DEFAULT entry
149
147
Execute the retrieved actions
End

FIG. 14

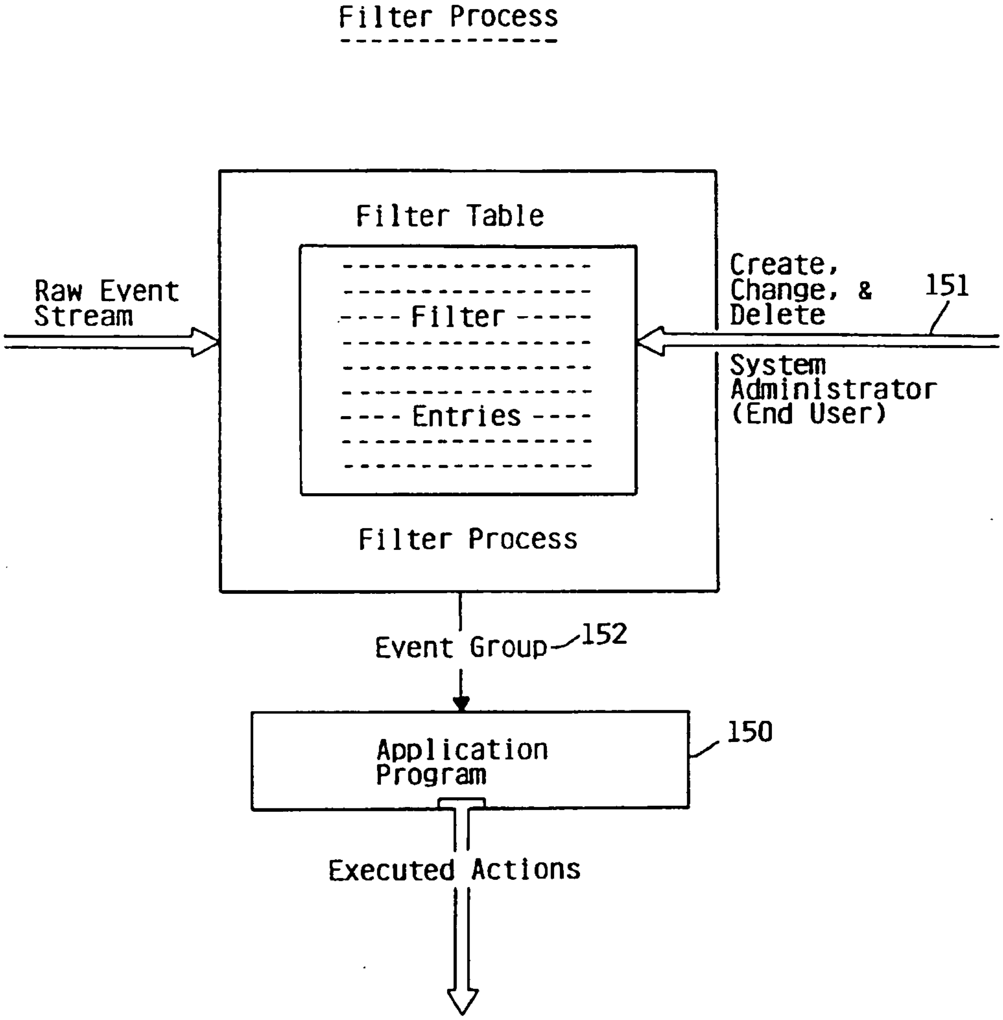

Filter Process
Filter Table
Filter
Entries
Filter Process
Raw Event Stream
Create, Change, & Delete
151
System Administrator (End User)
Event Group
152
Application Program
150
Executed Actions

FIG. 15